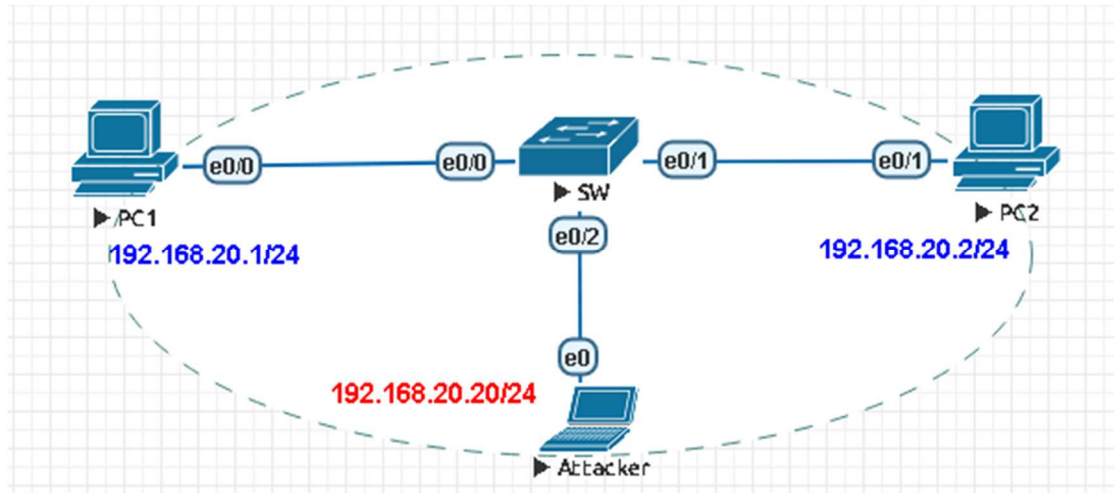


交换机 MAC 地址泛洪攻击的演示

一、拓扑



要求:

1. 演示 MAC 地址泛洪攻击，理解攻击的过程。
2. 配置防范 MAC 地址泛洪攻击的策略。

二、配置过程

1. IP 地址配置省略，在这里我们强调一下，其中攻击者采用 QEMU 镜像完成，其地址为 192.168.20.20/24。
2. 先完成网络的互通测试，并查看交换机的 MAC 表

```

C:\Documents and Settings\Administrator>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=7ms TTL=255
Reply from 192.168.20.1: bytes=32 time=2ms TTL=255
Reply from 192.168.20.1: bytes=32 time=2ms TTL=255
Reply from 192.168.20.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 7ms, Average = 3ms

C:\Documents and Settings\Administrator>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=3ms TTL=255
Reply from 192.168.20.2: bytes=32 time=2ms TTL=255
Reply from 192.168.20.2: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Documents and Settings\Administrator>

```

可以看到此时攻击者在连接到交换机上之后，可以访问局域网内的 PC1、PC2。这个过程在现实中很简单，只要局域网中的交换机有多余的接口，攻击者可以直接使用网线连接交换机即可。

当攻击者可以通过交换机在局域网中访问其它 PC 时，此时查看交换机的 MAC 表

```

SW#show mac address
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
20      5000.0001.0000   DYNAMIC   Et0/2
20      aabb.cc00.0300   DYNAMIC   Et0/0
20      aabb.cc00.0410   DYNAMIC   Et0/1
Total Mac Addresses for this criterion: 3
SW#show mac address aging-time
Global Aging time: 300
Vlan    Aging time
-----
SW#

```

可以发现交换机的 MAC 表中存在 3 个条目，其中第一条为攻击者的 MAC 和对应的接口。

现在为了完成 MAC 地址泛洪的演示，将 Aging-time 改为 3600S，这样方便查看 MAC 中的条目。

```

Sw(config)#mac address aging-time 3600
Sw(config)#end
Sw#show ma
*Dec 31 22:24:12.783: %SYS-5-CONFIG_I: Configured from console by console
Sw#show mac address
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
20      5000.0001.0000   DYNAMIC Et0/2
20      aabb.cc00.0300   DYNAMIC Et0/0
20      aabb.cc00.0410   DYNAMIC Et0/1
Total Mac Addresses for this criterion: 3
Sw#

```

3.在攻击者电脑上完成 MAC 地址泛洪的操作，即使用科来数据包生成器，通过修改攻击者发送的数据帧的源 MAC，让交换机收到该帧后，进行 MAC 地址的自动学习，从而将修改后的 MAC 地址和 e0/2 接口关联起来，加到 MAC 表中，我们在这里重复 10 次，完成 10 个 MAC 和 e0/2 的关联

①让源 MAC 为 aaaa:bbbb:0001

The screenshot shows a network packet capture tool interface. At the top, a table lists packet details: 1, 0.100000, AA:AA:BB:BB:00:01, FF:FF:FF:FF:FF:FF, ARP, 64, 谁是 192.168.20.50? ... Below this, the '数据包信息' (Packet Information) section is expanded to show '以太网 - II' (Ethernet II) and 'ARP - 地址解析协议' (ARP - Address Resolution Protocol) details. The source MAC address is highlighted as AA:AA:BB:BB:00:01.

再发送出去

200 - 200.200.200.200:46883 - 远程桌面连接

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.098800000	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
2	1.031242312	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
5	2.093724945	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
6	3.109497280	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
8	4.112692407	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
9	5.110811176	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
11	6.129580291	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
12	7.156378793	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
14	8.174068479	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
15	9.234456363	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20
17	10.237737274	aa:aa:bb:bb:00:01	Broadcast	ARP	60	Who has 192.168.20.50? Tell 192.168.20.20

可以看到 SW 从接口 e0/2 上不停的收到源 MAC 为 aa:aa:bb:bb:00:01 的帧。

接着查看交换机的 MAC 表

```
SW#show mac address
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
20      5000.0001.0000  DYNAMIC  Et0/2
20      aaaa.bbbb.0001  DYNAMIC  Et0/2
20      aabb.cc00.0300  DYNAMIC  Et0/0
20      aabb.cc00.0410  DYNAMIC  Et0/1
Total Mac Addresses for this criterion: 4
SW#
```

可以看到交换机此时已经学到了 aaaa.bbbb.0001 的 MAC 表项，与之关联的接口为 e0/2。

重复以上操作，直到演示如下：

```
SW#show mac address
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
20      5000.0001.0000  DYNAMIC  Et0/2
20      aaaa.bbbb.0001  DYNAMIC  Et0/2
20      aaaa.bbbb.0002  DYNAMIC  Et0/2
20      aaaa.bbbb.0003  DYNAMIC  Et0/2
20      aaaa.bbbb.0004  DYNAMIC  Et0/2
20      aaaa.bbbb.0005  DYNAMIC  Et0/2
20      aaaa.bbbb.0006  DYNAMIC  Et0/2
20      aaaa.bbbb.0007  DYNAMIC  Et0/2
20      aaaa.bbbb.0008  DYNAMIC  Et0/2
20      aaaa.bbbb.0009  DYNAMIC  Et0/2
20      aaaa.bbbb.000a  DYNAMIC  Et0/2
20      aabb.cc00.0300  DYNAMIC  Et0/0
20      aabb.cc00.0410  DYNAMIC  Et0/1
Total Mac Addresses for this criterion: 13
SW#
```

此时可以看到在 SW 的 MAC 表中，10 个不同的 MAC 地址对应于 e0/2 接口。

如果攻击者使用专业的攻击软件，在很短的时间内（小于交换机 SW 的 Aging-time）发送

数量极大(超出交换机的 MAC 表的容量)的不同源 MAC 的包,这样,就会使交换机的 MAC 表中全部充斥着和 e0/2 关联的 MAC 表项,而有关 PC1、PC2 的 MAC 表项,会被新的 MAC 表项挤出去。

此时,攻击者就完成了 MAC 地址泛洪的操作。

如果 PC1 和 PC2 相通信,PC1 发往 PC2 的二层数据帧到达交换机后,交换机查 MAC 表,发现 MAC 表中没有和 PC2 的 MAC 相关联的表项,此时只能进行未知帧的泛洪,即将该数据帧从除了 e0/0 (帧的接收接口)接口外的所有接口(必须和 e0/0 隶属于同一个 vlan)发送出去,当然,这也包含了 e0/2 接口,即攻击者所连的接口,这样,PC1 发往 PC2 的数据帧都会被攻击者收到——因为 SW 机把 PC1 发往 PC2 的所有数据帧进行了泛洪操作。

此时,交换机 SW 就相当于一台集线器。

这样,攻击者就可以轻松地窃取到该网段(同一 vlan)内的所有数据。

QQ:1186040994